L Number	Hits	Search Text	DB	Time stamp
1	90	@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and constant	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:02
2	505	(380/44).CCLS.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:02
3	279	(380/29).CCLS.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:02
5	25	((380/44).CCLS.) and ((380/29).CCLS.)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:02
6	119	@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and (shift$3 rotat$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:03
8	1	(("5442705").PN.) and (shift$3 rotat$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:20
9	71	@ad<19990831 and ("XOR" "exlusive-or" "exclusive or") and (key adj2 (transform$7 expan$5 exten$5)) and (shift$3 rotat$3) and (substitut$3 "s-box" "s-boxes")	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:04
10	0	(shift$3 rotat$3) near (relatively adj prime)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:20
11	0	(shift$3 rotat$3) and (relatively adj prime)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:20
12	0	relatively adj prime	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:20
13	316	relative$3 adj2 prime	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:20
14	222	relative$3 adj prime	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:21
15	222	relative$2 adj prime	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:21
16	0	relatively adj prime	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 14:21
17	0	"relatively prime"	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:04
18	6	"relatively prime"	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/02/26 15:19

21	84	"des" and (key adj expansion)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/02/26 15:20
22	45	"des" same (key adj expansion)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/02/26 15:20
19	7	"des" near (random adj3 generator)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/02/26 15:20
7	1	("5442705").PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:32
24	4111	(substitut$3 "s-box" "s-boxes") near ("same" common)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:53
28	2947	((substitut$3 "s-box" "s-boxes") near ("same" common)) and @ad<19990831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:50
29	203	(((substitut$3 "s-box" "s-boxes") near ("same" common)) and @ad<19990831) and (sharing shared share)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:53
32	9	((((substitut$3 "s-box" "s-boxes") near ("same" common)) and @ad<19990831) and (sharing shared share)) and (380/$.ccls.)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:52
33	23	@ad<19990831 and ((substitut$3 "s-box" "s-boxes") near (sharing shared share "same" common)) and (random near generat$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:55
34	1	(OOMORI and MOTOJI).in.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:56
35	52	(OhMORI and MOTOJI).in.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 15:56
36	25	(OhMORI and MOTOJI).in. and (toshiba matsushita).as.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 16:00
37	13	((OhMORI and MOTOJI).in. and (toshiba matsushita).as.) and @ad<20000831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 16:09
38	1	"EP 874496 A2"	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/26 16:10

Google Advanced Search Preferences Language Tools Search Tips

"key expansion" rotate DES Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **"key expansion" rotate DES**. Results **1** - **10** of about **104**. Search took

[PDF] Network Security: Secret Key Cryptography
File Format: PDF/Adobe Acrobat - View as HTML
... bit **rotate** left ¯ otherwise: two-bit **rotate** left ¯ permutation ... ETH Zurich, 1991 ¯ similar to **DES**: 64 bit ... 16 IDEA **Key Expansion** ¯ 128-bit key 52 16-bit keys ...
www.cs.columbia.edu/~hgs/teaching/ security/slides/secret1.pdf - Similar pages

[PDF] Network Security: Secret Key Cryptography Secret Key Cryptography
File Format: PDF/Adobe Acrobat - View as HTML
... bit **rotate** left ¯ otherwise: two-bit **rotate** left ¯ permutation ... ETH Zurich, 1991 ¯ similar to **DES**: 64 bit ... for ¾ ½ Slide 15 IDEA **Key Expansion** ¯ 128-bit ...
www.cs.columbia.edu/~hgs/teaching/ security/slides/secret2.pdf - Similar pages
[More results from www.cs.columbia.edu]

[PDF] William Stallings, Cryptography and Network Security 3/e
File Format: PDF/Adobe Acrobat - View as HTML
... keys • Stronger & faster than Triple-**DES** • Active life ... AES **Key Expansion** • Takes 128-bit (16-byte) key and ... every 4 th has S-box + **rotate** + XOR constant ...
www-courses.cs.uiuc.edu/~cs397pgn/lectures/AES.pdf - Similar pages

[PPT] William Stallings, Cryptography and Network Security 3/e
File Format: Microsoft Powerpoint 97 - View as HTML
... stronger & faster than Triple-**DES**. ... AES Round. AES **Key Expansion**. ... every 4th has S-box + **rotate** + XOR constant of previous before XOR together. ...
security.ece.orst.edu/koc/ece478/ws/slides/ch05.ppt - Similar pages

[PS] The MARS Encryption Algorithm Carolynn Burwick c , Don Coppersmith ...
File Format: Adobe PostScript - View as Text
... Our C implementation of the **key expansion** procedure sets up ... As a basis for comparison,
a typical **DES** implementation is ... odd integer) into R and then **rotate** R by ...
www.research.ibm.com/security/mars-short.ps - Similar pages

An Overview of the Hasty Pudding Cipher Rich Schroeppel & Hilarie ...
... by the operations that add, shift, and **rotate**, because the ... The cipher key controls the **key expansion** table at the ... a "step" is similar to a **DES** "round") that ...
www.cs.arizona.edu/~rcs/hpc/hpc-overview - 19k - Cached - Similar pages

[PDF] Microsoft PowerPoint - lect07.ppt
File Format: PDF/Adobe Acrobat - View as HTML

... Fall 2003/Lecture 7 21 **Key Expansion** RotWord([byte0, byte1, byte2 ... Speed: faster than **DES** in software. ... Every time more subkeys are needed, **rotate** left the key 25 ...
www.cs.purdue.edu/homes/ninghui/courses/ Spring04/lectures/lect07.pdf - Similar pages

[PDF] Lecture 6: Two Fish on the Rijndael Menu Breaking Grades File ...
File Format: PDF/Adobe Acrobat - View as HTML
... for S-boxes kept secret • Many good choices – **DES**: only one ... of key bytes: b (16, 24, or 32) • **Key Expansion**: – Produces array S ... n means **rotate** left by ...
www.cs.virginia.edu/~evans/cs588/lectures/lecture6.pdf - Similar pages

[PDF] Hardware Evaluation of the AES Finalists
File Format: PDF/Adobe Acrobat - View as HTML
... Twofish, Mars and RC6 are slower than Triple-**DES**. ... 4-bit input/output, logical and **rotate** shifts, and ... Decrypti on logic Output registers **Key Expansion** logic Su ...
csrc.nist.gov/encryption/aes/round2/ conf3/papers/15-tichikawa.pdf - Similar pages

[PPT] Testing in the Fourth Dimension
File Format: Microsoft Powerpoint 97 - View as HTML
... Stronger & faster than Triple-**DES**. ... CSE565: S. Upadhyaya. Lec 9.15. AES **Key Expansion**. ... every
4th has S-box + **rotate** + XOR constant of previous before XOR together. ...
www.cse.buffalo.edu/faculty/shambhu/ cse56503/lectures/lec-09-aes.ppt - Similar pages

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

"key expansion" rotate DES Google Search Search within results

Dissatisfied with your search results? Help us improve.

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help

Google Advanced Search Preferences Language Tools Search Tips

key (XOR OR "exclusive-or") (sul Google Search

Web · Images · Groups · Directory · News ·

Searched the web for **key (XOR OR "exclusive-or") (substitution OR "s-box") expansion (rotate OR rotation)**

The Dogfish Page
... transformation and is also performed, in combination with **substitution**, during **key**
expansion ... The Add Round **Key** transformation is performed by **XOR**'ing the ...

www.datacrime.org/ - 22k - Cached - Similar pages

BletchleyPark.net
... This operation consists of **substitution** boxes which specifies how each ... 192 or 256
bits and a complex **key expansion** process ... The **Xor**-ing of the sub-**key** before the ...
www.bletchleypark.net/crypt/aes.html - 20k - Cached - Similar pages

[PDF] William Stallings, Cryptography and Network Security 3/e
File Format: PDF/Adobe Acrobat - View as HTML
... **XOR** constant of previous before **XOR** together • Designed ... step – with a different
key schedule • Works ... is unchanged when – swap byte **substitution** & shift ...
www-courses.cs.uiuc.edu/~cs397pgn/lectures/AES.pdf - Similar pages

[PDF] AEES-Alex Ernst Encryption Standard
File Format: PDF/Adobe Acrobat - View as HTML
... 2. **Substitution** choice ... **S-box** S and it's inverse S -1 are applied in the law of ... bytes
of 8 in **XOR-Key** dwordS2 - second 4 bytes of 8 in **XOR-Key** dwordP2 - second ...
www.alex-encryption.de/DES_Cube_PRNG.pdf - Similar pages

[PPT] William Stallings, Cryptography and Network Security 3/e
File Format: Microsoft Powerpoint 97 - View as HTML
... every 4th has **S-box** + **rotate** + **XOR** constant of previous before **XOR** together. ... with
a different **key** schedule. ... swap byte **substitution** & shift rows. ...
security.ece.orst.edu/koc/ece478/ws/slides/ch05.ppt - Similar pages

From: pgut01@cs.auckland.ac.nz (Peter Gutmann) Newsgroups: sci. ...
... 2. Bitwise **exclusive OR**, denoted by ... random binary words determined by the user's secret
key K. Initialising ... ciphertext contents of Beale Cipher No.1 **XOR**'d with ...
www.funet.fi/pub/crypt/cryptography/symmetric/ rc2/comments/gutman-960211 - 10k - Cached - Similar pages

[PPT] Secret **Key** Cryptography

File Format: Microsoft Powerpoint 97 - View as HTML
... IDEA primitive operations. ® **exclusive OR** + addition mod 216 and x multiplication
mod 216+1. ... **XOR**. Octet-**Substitution** (**S-box**) (see Figure 3-24). ... **Key Expansion**. ...
www.cs.odu.edu/~mukka/cs772s04/slides/chapter3.ppt - Similar pages

Interest:
See your message here...

<html> <head> </head><body><pre><html> <head> &lt ...
... 2. Bitwise **exclusive OR**, denoted by "^&quot ... binary words determined by the user's secret **key** K. Initialising the **S-box** RRC.2 ...
www.mirrors.wiretapped.net/security/cryptography/ algorithms/rc2/comments/gutman-960211 - 11k - Cached - Similar pages

<html> <head> </head><body><pre><html> <head> &lt ...
... register Long r; /* Data value R(i-1) */ Long k; /* **Key** K(i) */ { Long a, b, c;
/* 32 bit **S-box** output, &amp ... amp; P output */ a = r ^ k; /* A = R(i-1) **XOR** K(i ...
www.mirrors.wiretapped.net/security/cryptography/ algorithms/loki/loki89.c - 13k - Cached - Similar pages
[More results from www.mirrors.wiretapped.net]

[PS] The MARS Encryption Algorithm Carolynn Burwick c , Don Coppersmith ...
File Format: Adobe PostScript - View as Text
... We denote by cA*da bitwise **exclusive-or** of the two words c ... We then multiply the second **key** word (constrained to contain ... Then we **xor** R into L, and also view the ...
www.research.ibm.com/security/mars-short.ps - Similar pages

Goooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

key (XOR OR "exclusive-or") (sul Google Search Search within results

Dissatisfied with your search results? Help us improve.

InfoSECURITYnetBASE

HOME | CONTACT US | PRICES

Search Our Site

Advanced Search

Information

- How it Works
- New Books
- How to Order
- Editors
- Technical Support
- Export Title List

Visit CRC Press Online!

Leading Publishers of Essential Information for the Professional and Technical Communities Worldwide!
CRC Press.

For Best Results

Use the latest versions of the software below. Click on the icons below to download for FREE.

Get Acrobat Reader

Microsoft Internet Explorer

Netscape NOW!

Searched for **"key expansion"** and found **2** documents
New Search

Search Results - 1 to 2
<< Back 1 Next >>

# Hits		Document	Book Title	Authors	Size
1	10	Chapter 9: Hash Functions and Data Integrity	Handbook of Applied Cryptography	Alfred J. Menezes Paul C. van Oorschot...	0.5 MB
2	2	Chapter 7: Block Ciphers	Handbook of Applied Cryptography	Alfred J. Menezes Paul C. van Oorschot...	0.5 MB

Search Results - 1 to 2
<< Back 1 Next >>